軟體加密與監管合規性：
可能存在重大安全風險的平價解決方案

監管與合規性要求

資料安全性在過去曾經僅被歸類為 IT 部門，但消費者資料外洩的情況持續發生，因此世界各國政府對企業提出的要求與日俱增，必須加密與保護所有可識別個人身份的資料。

從醫療保健的 HIPAA 到 EMEA 的 GDPR 以及加州的 CCPA，這些法規皆要求針對受保護的資料進行加密。在過去 3 年多以來，由於這些法規及其相關罰款和法律裁決風險持續飆升，合規性企業數目也以倍數增加。

隨著這些改變，IT 部門需要努力跟上資安維護的腳步，並面臨持續上漲的成本。在 COVID 疫情期間，預算用於投資額外的硬體和防火牆設備，卻犧牲了對於資料加密的關注。

事實上，使用 Microsoft BitLocker® 或是例如 Symantec、McAfee 以及其他公司的端點管理軟體進行軟體加密的情況正在增加中。有些企業和消費者也會使用一般 USB 隨身碟並另外搭配使用加密軟體。

加密和傳輸中的資料

員工和消費者有隨身攜帶其資料的需求。他們有一些選擇，例如使用：

1. 雲端服務：這個選擇很棒，能使用任何能連上網際網路的裝置來存取其資料。然而，此靈活性有其代價。雲端資料儲存讓使用者和公司降低其對資料的控管程度，並存在風險，尤其是我們看到的雲端伺服器是處於解鎖或已被存取的狀態。
2. 一般 USB 隨身碟：攜帶 USB 隨身碟好像更安全些，但 USB 隨身碟遺失而導致資料曝露的風險更大。舉例而言，遺失的 USB 隨身碟被發現內有機密資訊的故事比比皆是，或者自助洗衣店的抽屜中往往裝滿了遺失的 USB 隨身碟。
3. 加密型 USB 隨身碟：此類 USB 隨身碟內含硬體加密控制器和存取控制等客製化架構。一般使用 XTS 模式下最強大的 AES-256 位元加密來加密資料，並使用其他可能的保護措施，來減輕針對 USB 隨身碟實體和韌體的攻擊。此類 USB 隨身碟由專門從事安全裝置的公司所製造，雖然較一般 USB 隨身碟昂貴，但能提供更好的資料安全性。FIPS 197 或 FIPS 140-2 3 等級的 USB 隨身碟能帶給您更高等級的防護和安心感。
4. 具軟體加密功能的一般 USB 隨身碟：依法規要求並為了安全起見，使用具備 BitLocker 或其他工具的的軟體加密功能是不錯的選擇，這相對便宜並且提供同等於 AES-256 XTS 的加密。

毫無疑問地，在一般情況下，企業和產業內公司會傾向採用第 4 個選項：使用具軟體加密功能的一般 USB 隨身碟。主因是 BitLocker 或加密軟體某種程度上可視為「免費」的。

軟體加密並不符合監管合規性

對於企業安全專業人員而言，相較於較昂貴的硬體加密，軟體加密能提供完全相同程度的加密功能。但這是我們的選擇嗎？因企業的預算有限，出於合規性考量而轉向軟體加密，卻沒有意識到軟體加密的壞處。

軟體加密的 USB 隨身碟有何問題？靜態資料和傳輸中資料有進行 AES-256 XTS 加密嗎？通常而言，有的。但問題是：軟體加密被視為「可移除」的加密。

等等，可移除？這是否代表，使用者能關閉使用軟體加密 USB 隨身碟的加密功能？

答案正是如此。使用者可移除 USB 隨身碟中的軟體加密功能。您或許想問，為何要這樣做？這是因為，使用者單純只想存取檔案，而不使用密碼，或他們只是在需要使用 USB 隨身碟時忘記了密碼。

如何移除 USB 隨身碟中的軟體加密功能

對於不想輸入複雜密碼或其他密碼，來存取其資料的使用者而言，步驟很簡單：

1. 將軟體加密型 USB 隨身碟插入電腦
2. 將 USB 隨身碟格式化
3. 格式化之後，所有加密軟體就隨之被刪除
4. 將內含秘密或機密資訊的檔案複製到硬碟，就能輕易存取

使用者可以在使用不受限的電腦上輕易辦到此事，就算 IT 部門限制公司電腦使用格式化指令，仍然可以在非公司電腦上輕易完成。

考慮合規性目的，能輕易移除資訊加密，代表公司所提供的隨身碟目前未加密，一旦透過上述方式移除加密 (加密金鑰相關資料)，隨身碟中的加密資料就等於永遠遺失。移除加密後再複製到裝置上的資料，一律視作不安全且不合規，可能有違反 HIPAA、GDPR、CCPA 和其他規定的風險。

未加密隨身碟遺失的後果

假若一家公司所屬的 USB 隨身碟遺失後被找到，即便公司一開始不清楚公司的特殊合規要求，但後來透過社交媒體了解到，可能會要求其：

1. 進行取證調查並確認遺失的資料
2. 諮詢相關法律人員，確認是否發生違法行為
3. 確認是否需要通知客戶

這就是單一 USB 隨身碟遺失時，可能會變得非常昂貴的環節。律師諮詢費用通常為每小時數百美元，此類合規性諮詢的過程可能需要數千美元的花費。除了潛在的罰款、客戶與其他方的法律訴訟，還有資料曝露事件所帶來的窘境。

考慮實行低成本軟體加密的當下，並不會考慮這些風險和高昂的財務費用。

在公司網路上允許使用未加密 USB 隨身碟，還有另一種風險，我們通常稱之為「BadUSB」。BadUSB 是一種惡意軟體，不良行為者使用它來破壞公司防火牆，並透過 USB 儲存裝置，將惡意軟體滲透進公司的網路防護系統。

BadUSB

當 USB 隨身碟插入電腦時，電腦的晶片控制器就透過韌體來啟動 USB 隨身碟控制器並執行傳輸協定。此類傳輸甚至會在作業系統 (例如 Microsoft/macOS/Linux) 發現 USB 隨身碟已連接至系統之前就執行每個 USB 隨身碟都有插入 USB 連接埠時可執行動作的韌體。

駭客會利用這種傳輸機制，將惡意軟體滲透進去；方法是將 USB 隨身碟上的韌體替換成另一個惡意韌體。當目標電腦系統與 USB 隨身碟進行傳輸時，便可將惡意軟體滲透到目標電腦系統中。一般 USB 隨身碟對其控制器所執行的內部韌體並無安全性可言，因此 BadUSB 應運而生。可以說是「優良」的 USB 隨身碟被當作武器來滲透防火牆，並破壞網路防護。

許多公司試圖禁止在其系統上使用 USB 隨身碟，甚至用環氧樹脂把 USB 連接埠封起來。然而，他們發現員工還是需要 USB 隨身碟來隨身攜帶資料。例如，主管想要隨身攜帶資料並工作，或是將資料提供給公司雲端外的外部法律或財務顧問；需要取得資料才能進行工作，但無法存取公司資料庫的公司承包商；急於完成每月財務報表，並需要在家處理試算表格的財務分析師。

正如上述分析所示，使用此類一般 USB 隨身碟和軟體加密的解決方案，存在著重大風險。乍看之下便宜的東西，實際上可能很有害，而且更加昂貴。光是與律師就潛在資料外洩問題進行諮詢 2 至 3 個小時，就高過使用便宜解決方案所省下的費用。

硬體加密型 USB 隨身碟是符合監管合規性的最佳選擇

硬體加密型 USB 隨身碟成為符合監管合規性最佳選擇的原因：

1. 硬體加密型 USB 隨身碟的加密功能永遠是啟動狀態：使用者無法停用加密、重設密碼規則 (長度、複雜性)，並禁用自動密碼重試。不像軟體加密，軟體加密無法防範以字典攻擊進行重複嘗試密碼攻擊，硬體加密會限制重試次數，並在第 10 次密碼輸入錯誤 (或次數更少) 時鎖定資料。這在電腦廣泛運用的時代中是非常安全的選擇。
2. 硬體加密型 USB 隨身碟使用高階加密控制器，並具備眾多安全性功能：我們一般不會揭露太多安全對策，但在此分享一個防範 BadUSB 的對策。出廠前，硬體加密型 USB 隨身碟僅載入韌體時，韌體就會執行數位簽章並載入。這代表將硬體加密型 USB 隨身碟插入電腦時，加密控制器會先透過數位簽章來檢查韌體的完整性，通過驗證後才會進行載入。任何替換韌體的嘗試都無法正常啟用隨身碟，隨身碟無法正常執行，就沒有威脅。
3. 硬體加密型 USB 隨身碟能為指定公司設定客製化產品 ID (PID)：這些高階隨身碟能以程式寫入一個數位識別碼，如此一來，當隨身碟插入公司防火牆內外的裝置時，就可以識別出這是該公司所屬的隨身碟。舉例而言，如果員工遺失公司所屬的隨身碟，並在電腦零售店鋪購買了相同型號的隨身碟，那麼新購入的隨身碟將無法通過公司網路的驗證。使用此類客製化 USB 隨身碟，就能增加另一層安全性。
4. 硬體加密型 USB 隨身碟能快速地節省成本：光是降低和消除風險，就能讓投資回收週期變得很短。

Kingston 是全球最大加密型 USB 隨身碟製造商，提供各種功能和價格帶的隨身碟系列。直接與 Kingston 聯絡，探討我們如何協助您遵守合規性，並適用於主管、員工和承包商等人的加密型 USB 隨身碟製解決方案。